JOURNAL OF COMBINATORIAL THEORY (B) 15, 12–17 (1973)

Point-Symmetric Graphs and Digraphs of Prime Order and Transitive Permutation Groups of Prime Degree*

BRIAN ALSPACH

Simon Fraser University, Burnaby 2, British Columbia, Canada

Communicated by Frank Harary

Received June 6, 1972

In this paper the following two problems are solved: Given any point-symmetric graph or digraph Γ of prime order the automorphism group of Γ is explicitly determined and given any transitive permutation group G of prime degree p the number of digraphs and graphs of order p having G as their automorphism group is determined.

1. INTRODUCTION

A *graph* consists of a finite set of points V and a set of *lines* each of which joins two distinct points of V and no two lines join the same pair of points. If points u and v are joined by a line we say they are adjacent. A *directed graph*, hereafter called *digraph*, consists of a finite set of points V and a subset of the set of all ordered pairs (u, v), $u, v \in V$ and $u \neq v$. The ordered pairs (u, v) of the digraph are called *arcs*. If the arc (u, v) is in the digraph we say u dominates v.

In the case that the arc (u, v) is in the digraph Γ if and only if the arc (v, u) is also in Γ, we can replace Γ by the corresponding graph Γ' in which u is adjacent to v if and only if the pair of arcs (u, v) and (v, u) are in Γ. Clearly Γ and Γ' have the same automorphism group and throughout this paper we obtain results about graphs from results about digraphs by thinking of such a digraph Γ as the corresponding graph Γ'.

A digraph or graph Γ is said to be *point-symmetric* (*symmetric*) if the automorphism group of Γ, denoted $\mathcal{A}(\Gamma)$, acts transitively on the points (both the points and arcs or lines) of Γ. The notation PPS digraph (graph) will be used to denote a point-symmetric digraph (graph) of prime order. Z_p will denote the integers modulo p while $Z_p^* = Z_p - \{0\}$.

* This research was sponsored by NRC Grant A-4792.

In [8] it is shown that for every PPS graph Γ with points $v_0, v_1, \ldots, v_{p-1}$ there exists a set $S \subseteq Z_p^*$ such that $a \in S \Rightarrow p - a \in S$ and v_i and v_j are adjacent in Γ if and only if $j - i \in S$ (here and throughout this paper operations on subscripts are taken modulo p). S is called the *symbol* of Γ. The methods of [8] apply equally well to digraphs so that the symbol S of a PPS digraph is defined analogously. However, the symbol S of a PPS digraph need not satisfy $a \in S \Rightarrow p - a \in S$. It is also shown in [8] that two PPS digraphs or graphs Γ and Γ' with respective symbols S and S' are isomorphic if and only if $S' = Sa = aS$ for some $a \in Z_p^*$. The preceding result is useful in the following material.

Since Z_p^* is cyclic the following notation makes sense. If S is the symbol of a PPS digraph Γ, let $D(S)$ denote the largest subgroup H of Z_p^* such that S is a union of cosets of H and if S is the symbol of a PPS graph Γ, let $E(S)$ denote the largest even order subgroup H of Z_p^* such that S is a union of cosets of H.

We shall use $\leqslant$ and $<$ to denote subgroup and proper subgroup containment throughout this paper.

2. The Groups of the Digraphs

The following theorem is the basis for the main results of this paper. It is simply the digraph analog of the main result of [1] and the identical proof used in [1] proves our Theorem 1.

THEOREM 1. *A non-trivial* PPS *digraph Γ of order p is symmetric if and only if its symbol S is a coset of a subgroup $H \leqslant Z_p^*$. Moreover, if $H < Z_p^*$, then $\mathcal{A}(\Gamma) = \{T_{a,b} : a \in H, b \in Z_p\}$ where $T_{a,b}(v_i) = v_{ai+b}$, $i = 0, \ldots, p-1$. If $S = Z_p^*$, then $\mathcal{A}(\Gamma) = S_p$, the symmetric group of degree p.*

The graph analog of Theorem 1 differs from Theorem 1 only in that H must be an even order subgroup of Z_p^*.

THEOREM 2. *Let Γ be a* PPS *digraph (graph) of order p with symbol S. If $S = \varnothing$ or $S = Z_p^*$, then $\mathcal{A}(\Gamma) = S_p$, the symmetric group of degree p. Otherwise, $\mathcal{A}(\Gamma) = \{T_{a,b} : a \in H, b \in Z_p\}$ where $H = D(S) (H = E(S))$.*

Since $H < Z_p^*$ and S is a union of cosets of H, $|H|$ must divide the g.c.d. of $|S|$ and $p - 1$, denoted $(p - 1, |S|)$. This proves the following two corollaries:

COROLLARY 2.1. *If Γ is a* PPS *digraph of order p with symbol S and if $(p - 1, |S|) = 1$, then $\mathcal{A}(\Gamma)$ is the cyclic group C_p of order p.*

COROLLARY 2.2. *If Γ is a* PPS *graph of order p with symbol S and if $(p-1, |S|) = 2$, then $\mathcal{A}(\Gamma) = D_p$, the dihedral group of degree p.*

EXAMPLE. Let Γ be the PPS graph of order 29 with symbol $S = \{1, 3, 5, 12, 17, 24, 26, 28\}$. By the above remark $|H| = 1, 2$, or 4. The latter two subgroups of Z_{29}^* are $\{1, 28\}$ and $\{1, 12, 17, 28\}$. With little work it can be seen that S is a union of four cosets of $\{1, 28\}$ and not a union of two cosets of $\{1, 12, 17, 28\}$. By Theorem 2 we have $\mathcal{A}(\Gamma) = \{T_{a,b} : a = 1, 28 \text{ and } b \in Z_{29}\}$, that is, $\mathcal{A}(\Gamma)$ is the transitive subgroup of S_{29} of order 58. The definite article in the preceding sentence is appropriate because of a classical theorem of Burnside [5, Thm. 7.8] which implies that all transitive subgroups of S_p, p a prime, of the same order n, $n \leqslant p(p-1)$, are conjugate.

Let Q_p, p a prime, denote the *quadratic residue digraph* of order p defined by a dominates b if and only if $b - a \in Q(p)$ where $Q(p)$ denotes the set of quadratic residues modulo p. If $p \equiv 1 (\mathrm{mod}\ 4)$, then Q_p is, in fact, a graph while, if $p \equiv 3 (\mathrm{mod}\ 4)$, then Q_p is a tournament. The following corollary for $p \equiv 3 (\mathrm{mod}\ 4)$ is a special case of the main result of [4].

COROLLARY 2.3. *If Q_p is the quadratic residue digraph of order p, p a prime, then $\mathcal{A}(Q_p) = \{T_{a,b} : a \in Q(p)$ and $b \in Z_p\}$ and $|\mathcal{A}(Q_p)| = p(p-1)/2$.*

3. ENUMERATION RESULTS

In [3] the problem of enumerating the graphs and digraphs of order n whose automorphism group is either the dihedral group D_n or the cyclic group C_n generated by a cycle of length n was posed. It was solved for n a prime in [7]. We now solve the corresponding problem for any transitive subgroup of S_n when n is a prime.

For $G \leqslant S_n$ let $\eta(G)$ and $\mu(G)$ denote the number of digraphs and graphs, respectively, of order n having G as their automorphism group. Even determining whether or not $\eta(G) > 0$ and $\mu(G) > 0$ for arbitrary $G \leqslant S_n$ is largely unsolved. We now turn to transitive $G \leqslant S_n$. If $G < S_n$ is doubly transitive, then $\eta(G) = \mu(G) = 0$ while $\eta(S_n) = \mu(S_n) = 2$. From Theorem 1, its graph analog and Burnside's Theorem [5, Th. 7.8] which states that, if $G \leqslant S_p$, p a prime, is transitive, then either G is doubly transitive or $G \cong \{F_{a,b} : a \in H < Z_p^*, b \in Z_p\}$ where $F_{a,b}(x) = ax + b$ for $x \in Z_p$, we can prove the following result by choosing H as the symbol of a digraph or graph of order p.

THEOREM 3. *If $G < S_p$, p a prime, is transitive, then $\eta(G) > 0$ if and only if G is not doubly transitive ($\mu(G) > 0$ if and only if G is not doubly transitive and $|\ G\ |$ is even).*

Let F_m denote the cycle index (see [2]) of the cyclic permutation group generated by an m-cycle. Thus

$$F_m = \frac{1}{m} \sum_{d|m} \phi(m/d)\, x_{m/d}^{d}$$

where ϕ is the Euler ϕ-function. Let $F_m(\bar{2})$ denote the value of F_m with each $x_i = 2$, $i = 1,\ldots, m$.

THEOREM 4. *Let $G < S_p$, p a prime, be transitive with $G = \{F_{a,b} : a \in H < Z_p{}^*, b \in Z_p\}$. Let $s = (p-1)/|\ H\ |$ and $\mathscr{P}$ denote the set of distinct primes occurring in the factorization of s with $|\ \mathscr{P}\ | = k$. Then*

$$\eta(G) = F_s(\bar{2}) - \sum_{q \in \mathscr{P}} F_{s/q}(\bar{2}) + \cdots + (-1)^t \sum_{A(t) \subseteq \mathscr{P}} F_{s/\pi A(t)}(\bar{2}) + \cdots + (-1)^k F_{s/\pi A(k)}$$

where $A(t)$ denotes a subset of $\mathscr{P}$ of order t and $\pi A(t)$ denotes the product of the elements of $A(t)$.

If $|\ G\ |$ is even, then $|\ H\ |$ is even and if Γ is a digraph of order p such that $\mathscr{A}(\Gamma) = G$, then by Theorem 2 its symbol S is a union of cosets of H in $Z_p{}^*$. Hence, $s \in S \Rightarrow p - s \in S$ so that Γ is really a graph in disguise. These remarks and Theorem 3 prove the next corollary.

COROLLARY 4.1. *If $G < S_p$, p a prime, is transitive but not doubly transitive, then $\mu(G) = 0$ if $|\ G\ |$ is odd and $\mu(G) = \eta(G)$ if $|\ G\ |$ is even.*

EXAMPLE. Let C_{29} denote the cyclic group of order 29 in S_{29}. Here $|\ H\ | = 1$, $s = 28$, and $\mathscr{P} = \{2, 7\}$. Then

$$\eta(C_{29}) = F_{28}(\bar{2}) - F_{14}(\bar{2}) - F_4(\bar{2}) + F_2(\bar{2}) = 9{,}587{,}580 - 1{,}182 - 6 + 3 = 9{,}586{,}395.$$

4. PROOFS OF THEOREMS 2 AND 4

We now prove Theorem 2. If $S = Z_p{}^*$ or $S = \phi$, then Γ is the complete digraph of order p or its complement and $\mathscr{A}(\Gamma) = S_p$ as asserted. Suppose $\phi \subset S \subset Z_p{}^*$. By Burnside's Theorem [5, Th. 7.8] $\mathscr{A}(\Gamma) =$

$\{T_{a,b} : a \in H < Z_p^*, b \in Z_p\}$. S is simply the set of indices of the points dominated by v_0 and the stabilizer of v_0, denoted $\mathcal{A}(\Gamma)_0$, is $\mathcal{A}(\Gamma)_0 = \{T_{a,0} : a \in H\}$. For $s \in S$ we have $\mathcal{A}(\Gamma)_0(s) = Hs \subseteq S$ and S is a union of cosets of H. Now S cannot be a union of cosets of K with $H < K$ or else $\mathcal{A}(\Gamma) \geqslant \{T_{a,b} : a \in K, b \in Z_p\}$ by Theorem 1 and the fact that two PPS digraphs each having a coset of K as their symbol have identical automorphism groups. Thus $H = D(S)$. The proof for a PPS graph is exactly the same.

We now prove Theorem 4. From Theorem 2 we know $\mathcal{A}(\Gamma) \geqslant G$ if the symbol of Γ is a union of cosets of H. On the other hand, if $\mathcal{A}(\Gamma) \geqslant G$ and $\mathcal{A}(\Gamma) \neq S_p$, then again by Burnside's Theorem $\mathcal{A}(\Gamma) = \{T_{a,b} : a \in K < Z_p^*, b \in Z_p\}$ and the symbol of Γ is a union of cosets of K. But Z_p^* is cyclic so that $K \geqslant H$ and thus the symbol of Γ is a union of cosets of H. Hence, $\mathcal{A}(\Gamma) \geqslant G$ if and only if the symbol of Γ is a union of cosets of H. Recall that two PPS digraphs Γ and Γ' with respective symbols S and S' are isomorphic if and only if $S' = Sa$ for some $a \in Z_p^*$. These right multiplications induce a cyclic permutation group on the cosets of H in Z_p^* that is generated by a cycle of length s. Consequently, by Pólya's Theorem [2, Th. 5.1], $F_s(\bar{2})$ is the number of PPS digraphs of order p whose symbols are unions of cosets of H, that is, the number of PPS digraphs Γ of order p such that $\mathcal{A}(\Gamma) \geqslant G$.

Choose any t distinct primes $\{p_1, \ldots, p_t\} = A(t)$ in $\mathcal{P}$ and let $|H| = h$. Then $F_{s/\pi A(t)}(\bar{2})$ is the number of PPS digraphs Γ of order p such that $\mathcal{A}(\Gamma) \geqslant \{T_{a,b} : a \in K < Z_p^*, b \in Z_p, |K| = h\pi A(t)\}$. Hence, by inclusion-exclusion, in the expression for $\eta(G)$ every Γ of order p for which $\mathcal{A}(\Gamma)$ properly contains G has been counted zero times. This completes the proof.

In the preceding proof of Theorem 4 one sees how to enumerate the digraphs (or graphs) of order p having G as their automorphism groups and each point having a prescribed outdegree n. Using Pólya's store enumerator [2] the coefficient of x^r in $F_{s/\pi A(t)}(x + y, x^2 + y^2, x^3 + y^3, \ldots)$ is the number of digraphs Γ of order p such that $\mathcal{A}(\Gamma) \geqslant \{T_{a,b} : a \in K < Z_p^*, b \in Z_p, |K| = h\pi A(t)\}$ and each point has outdegree (and indegree) $rh\pi A(t)$. Therefore, if for each term in the expression for $\eta(G)$ we make the substitution

$$F_{s/\pi A(t)}(x^{1/h\pi A(t)} + y^{1/h\pi A(t)}, x^{2/h\pi A(t)} + y^{2/h\pi A(t)}, \ldots) \quad \text{for} \quad F_{s/\pi A(t)},$$

then the coefficient of x^n in the final expression is the desired number of digraphs.

We wish to thank the referee for pointing out to us that Theorem 2 and some of the results in the references also can be obtained from [6, Thm. 2].

REFERENCES

1. J. L. BERGGREN, An algebraic characterization of symmetric graphs with p points, p an odd prime, *Bull. Austral. Math. Soc.* **7** (1972), 131–134.
2. N. G. DE BRUIJN, Pólya's theory of counting, "Applied Combinatorial Mathematics," Ch. 5, Wiley, New York, 1964.
3. B. ELSPAS AND J. TURNER, Graphs with circulant adjacency matrices, *J. Combinatorial Theory* **9** (1970), 297–307.
4. M. GOLDBERG, The group of the quadratic residue tournament, *Canad. Math. Bull.* **13** (1970), 51–54.
5. D. S. PASSMAN, "Permutation Groups," Benjamin, Menlo Park, Calif., 1968.
6. G. SABIDUSSI, Vertex-transitive graphs, *Monatsh. Math.* **68** (1964), 426–438.
7. P. K. STOCKMEYER, Enumeration of graphs with prescribed automorphism group, Ph.D. Dissertation, University of Michigan, 1971.
8. J. TURNER, Point-symmetric graphs with a prime number of points, *J. Combinatorial Theory* **3** (1967), 136–145.